UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,684	01/04/2007	Yuichi Futa	2006_0401A	3546

52349 7590 09/08/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/573,684	FUTA ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/27/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/573684 filed on 3/27/06 is presented for examination by the examiner.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Specification

The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01. Hyperlinks were found on page 2, lines 2 and 18-19 and on page 23, line 11.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 12 is rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, per se. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor is it a combination of chemical

compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material per se.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").See MPEP 2106.01 [R-6].

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 4, the hash value cannot be the same as the hash value of claim 3. In claim 4, as it is interpreted by the Examiner, the hash key is obtained from the hash value. However, in claim 3, the hash value is obtained using the hash key. This implies the hash key already exists at a time prior to the hash value being created. This contradicts claim 4's hash value that is intended to be the same hash value of claim 3. This also raises the question as to the number of hash value. Examiner could not find support for such a method using more than one hash value in the specification. For purposes of examination, claim 4 is being interpreted to read as claim 5, the key difference being the concatenation of the 1st and 2nd keys as opposed to the exclusive OR operation in claim 5. Appropriate correction is required.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 7, and 10-13 are rejected under 35 U.S.C. 102(b) as being anticipated by USP 5,371,794 to Diffie et al., hereinafter Diffie.

As per claim 1, Diffie teaches device and a second device, wherein the first device [base] (i) encrypts a 1st key [RN1] using a public key of the second device [mobile] to generate 1st encrypted data, and transmits the 1st encrypted data to the second device (Fig. 5a),

(ii) receives 2nd encrypted data from the second device, and decrypts the 2nd encrypted data using a secret key of the first device to obtain a 2nd key [RN2], and (Fig. 5a)

(iii) generates, based on the 1st and 2nd keys, a 1st encryption key [session key] for use in communication with the second device, the second device (Fig. 5b)

(i) encrypts a 3rd key [RN2] using a public key of the first device to generate the 2nd encrypted data, and transmits the 2nd encrypted data to the first device (Fig. 5a),

(ii) receives the 1st encrypted data from the first device, and decrypts the 1st encrypted data using a secret key of the second device to obtain a 4th key [RN1] (Fig. 5a), and

(iii) generates, based on the 3rd and 4th keys, a 2nd encryption key [session key] for use in communication with the first device (Fig. 5a), and the first and second devices perform encrypted communication using the 1st and 2nd encryption keys (Fig. 5b).

As per claims 2, 11, 12, and 13, Diffie teaches a data generation unit operable to encrypt a 1st key [RN1] using a public key that corresponds to a secret key held by the other device to generate 1st encrypted key data, and transmit the 1st encrypted key data to the other device (Fig. 5a);

a decryption unit operable to receive, from the other device, 2nd encrypted key data generated by the other device encrypting a 3rd key [RN2] using a public key of the communication device, and decrypt the 2nd encrypted key data using a secret key of the communication device to obtain a 2nd key [RN2] (Fig. 5a);
a key generation unit operable to generate an encryption key [session key] based on the 1st and 2nd keys (Fig. 5b); and
a communication unit operable to perform encrypted 15 communication with the other device using the encryption key (Fig. 5b).

As per claim 7, Diffie teaches an authentication unit operable to authenticate the other device, using the encryption key (col. 15, line 50).

As per claim 10, Diffie teaches the data generation [packet] unit encrypts the 1st key [RN1] based on a key encapsulation mechanism to generate the 1st encrypted key data, and the decryption unit decrypts the 2nd encrypted key data based on a key decryption mechanism to obtain the 2nd key [RN2] (col. 9, lines 57-63).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 5, and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie in view of USP Application Publication 2003/0204743 to Devadas et al., hereinafter Devadas.

As per claim 3, Diffie teaches an encryption subunit operable to encrypt the transmission data using the encryption key to generate encrypted data (Fig. 5b). Diffie is silent in explicitly teaching the key generation unit further generates a hash key based on the 1st and 2nd keys, and a calculation subunit operable to calculate, using the hash key, a hash value for transmission data; and transmitting the hash value with the encrypted data to the other device. Devadas teaches the key generation unit further generates a hash key based on the encryption key [secret key], and a calculation subunit operable to calculate, using the hash key, a hash value for transmission data; and transmitting the hash value with the encrypted data to the other device (0212). Diffie uses the two parts of the keys to form a session key whereby data is encrypted. Devadas uses a encryption key or session key as a MAC key [hash key]. The MAC then hashes message with the encryption key to produce an encrypted message with a hash value. Devadas uses this known method of message authentication code to further secure the data packet during transmission. This MAC prevents tampering of

the packets. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the known method of MAC with the teaching of Diffie because it would increase the security of the system. It is obvious to incorporate other known security measures to strengthen a system.

As per claim 5, the combined system of Diffie and Devadas teaches the key generation unit performs an exclusive OR operation using the 1st and 2nd keys (Diffie, col. 8, lines 47), and generates the encryption key and the hash key based on a result of the operation. Diffie XOR's the key parts to create the session key. Examiner relies on the rationale to combine Devadas and Diffie as disclosed above for using a hash key.

As per claim 6, Diffie does not explicitly teach the key generation unit further generates a hash key based on the 1st and 2nd keys,
the communication unit includes:
a receiving subunit operable to receive, from the other device, encrypted data generated by encrypting data using an encryption key held by the other device, and a 1st hash value calculated for the data using a hash key held by the other device; a decryption subunit operable to decrypt the encrypted data using the encryption key to obtain plaintext data; and
a judging subunit operable to calculate a 2nd hash value for the plaintext data using the hash key, and judge whether the first and second hash values match, and
the communication device further includes a usage unit operable to use the plaintext data if the hash values are judged to match, and to suppress use of the plaintext data

if the hash values are judged not to match. Examiner relies on the above rationale for combining Diffie with Devadas to incorporate the hash key and creating a MAC. Devadas also teaches using the encrypted data generated by encrypting data using an encryption key held by the other device, and a 1st hash value calculated for the data using a hash key held by the other device; a decryption subunit operable to decrypt the encrypted data using the encryption key to obtain plaintext data; and
a judging subunit operable to calculate a 2nd hash value for the plaintext data using the hash key, and judge whether the first and second hash values match, and
the communication device further includes a usage unit operable to use the plaintext data if the hash values are judged to match, and to suppress use of the plaintext data if the hash values are judged not to match [0212]. Devadas uses a MAC so that when packets are received the received MAC can be compared to a calculated MAC by using a the key to decrypt the message. Once the message is decrypted, the message can be passed through the MAC and this output is compared to the sent MAC. Again this is a known method of authenticating data thereby preventing tampering. Examiner replies on the same rationale that is it obvious to combine known cryptographic functions to strength the overall security of the system. One of ordinary skill in the art knows the use of MACs. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate verifying the authenticity of the MACs.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie and Devadas as applied to claim 2 above, and further in view of USP Application Publication 2003/0093669 to Morais et al., hereinafter Morais.

As per claim 4, Diffie and Devadas do not explicitly teach the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value. Morais teaches the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value [0052]. Diffie and Devadas teach using XOR to combine the key parts. Concatenation as taught by Morais of key parts is yet another way to logically combine keys to arrive at another key. This is just a simple substitution of a known function and as such it would have been obvious to one of ordinary skill at the time the invention to substitute another known logical way of combining keys. The combining rationale of Diffie and Devadas is again relied upon to use the newly formed encryption and hash key to generate hash values (MAC). Examiner reasserts the interpretation of claim 4 as disclose under the *35 USC § 102* rejection.

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie in view of USP Application Publication 2003/0041253 to Matsui et al., hereinafter Matsui.

As per claim 8, Diffie is silent in teaching the authentication unit (i) generates a 1st authentication value, encrypts the 1st authentication value using the encryption key to generate a 1st encrypted value, and transmits the 1st encrypted value to the other device, and (ii) receives, from the other device, a 2nd authentication value generated by decrypting the 1st encrypted value using an encryption key held by the other device, and judges whether the 1st and 2nd authentication values match, and the communication device further comprises a communication unit operable to perform communication with the other device if the authentication values are judged to match. Matsui teaches the authentication unit (i) generates a 1st authentication value, encrypts the 1st authentication value using the encryption key to generate a 1st encrypted value, and transmits the 1st encrypted value to the other device, and (ii) receives, from the other device, a 2nd authentication value generated by decrypting the 1st encrypted value using an encryption key held by the other device, and judges whether the 1st and 2nd authentication values match, and the communication device further comprises a communication unit operable to perform communication with the other device if the authentication values are judged to match [0052]. Matsui teaches the method of mutual authentication to decrease the chance of an impersonator acting maliciously and stealing information. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further strengthen the security of Diffie by authenticating both parties through the use of the encryption key. An attacker would have to know both parts of the key in order to

break this authentication scheme. It also insures that both parties have correctly arrived at the same key and therefore encryption communication can proceed.

As per claim 9, Diffie is silent in teaches the authentication unit receives, from the other device, a 3rd encrypted value generated by encrypting a 3rd authentication value using the encryption key held by the other device, decrypts the 3rd encrypted value using the encryption key to obtain a 4th authentication value, and transmits the 4th authentication value to the other device, and the communication unit performs the communication if the other device judges the 3rd and 4th authentication values to match. Matsui teaches the other half of the mutual authentication method in [0053]. Examiner relies upon the above rationale for combining Diffie and Matsui and the obviousness of mutual authentication through the use of a encryption key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2131

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131